

**AMENDMENTS TO THE CLAIMS**

The following is a complete, marked-up listing of revised claims with a status identifier in parenthesis, underlined text indicating insertions, and strike through and/or double-bracketed text indicating deletions.

**LISTING OF CLAIMS**

1. (Currently Amended) ~~Pairing Control~~ A pairing control method between a first device such as a removable security module and a second device such as a host apparatus, ~~this the~~ pairing control method aiming to secure the data exchange with the aid of a unique pairing key, ~~this the pairing control method comprising the steps of:~~

- verifying the pairing between the two devices and using the unique pairing key if the pairing has been already carried out, if not,

- searching for a free location among the locations reserved for the pairing data in the first device and in this case,

- initiating a pairing procedure by transmitting a cryptogram contained in the second device, and comprising an identifier belonging to ~~this the second device~~, this the cryptogram being encrypted by a secret key common to all the first devices,

- decrypting ~~this the~~ cryptogram with the first device and extracting from ~~this the~~ cryptogram the identifier of the second device,

- generating a pairing key based on ~~this the~~ identifier,

- ~~storing in the first device the pairing data with the second device~~ storing the pairing key in the first device, the pairing key used to pair with the second device.

2. (Currently Amended) ~~Method~~ The method according to claim 1, wherein the pairing key is based on the identifier of the second device and on the data of the first device.

3. (Currently Amended) ~~Method~~The method according to claim 1, wherein the cryptogram is stored in the first device and encrypted with a secret key common to a plurality of~~the~~ second devices.
4. (Currently Amended) ~~Method~~The method according to claim 1, wherein each location includes an activity counter updated during every positive verification of the pairing based on this location, the search for the location to be replaced being determined by the value of the activity counter.
5. (Currently Amended) ~~Method~~The method according to claim 1, wherein pairing is conditioned by the introduction of a secret code transmitted to the first device and verified by said first device.
6. (Currently Amended) ~~Method~~The method according to claim 5, wherein the secret code belongs to and is unique to each first device.
7. (Currently Amended) ~~Method~~The method according to claim 5, wherein the required secret code is different in each pairing.
8. (Currently Amended) ~~Method~~The method according to claim 5, ~~wherein it comprises the steps of~~ further comprising:
  - transmitting a unique identifier of the first device and a unique identifier of the second device to a management centre,

- verifying the conformity of this pairing and calculating by means of the management centre the corresponding secret code on the basis of the two identifiers,
- transmitting this secret code to the user,
- initiating the pairing and requesting the introduction of the secret code, by means of the first device,
- calculating by means of the first device the necessary secret code on the basis of the identifiers of the first and second devices,
- comparing the calculated code with that which has been introduced by the user,
- accepting the pairing if the two codes are identical.

9. (Currently Amended) ~~Method~~The method according to claim 8, ~~wherein it comprises the step of further comprising,~~ determining the new secret code on the basis of the two identifiers and of an index that represents the number of pairings previously carried out, whereas the first device stores this index in its memory.

\*\*\* END CLAIM LISTING \*\*